PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-166996
(43)Date of publication of application : 22.06.2001

(51)Int.CI. G06F 12/14
G09C 1/00
G11B 20/10
H04L 9/10
H04L 9/32

(21)Application number : 2000-252462
(22)Date of filing : 23.08.2000

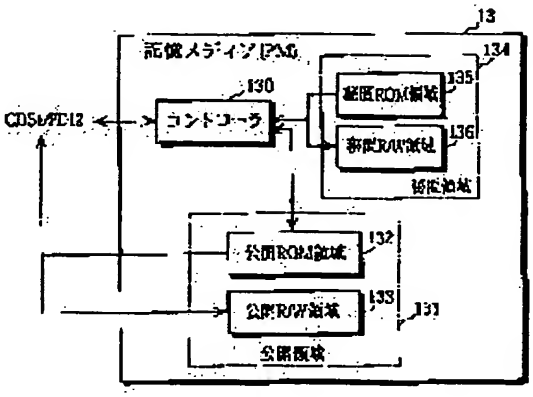
(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
TOSHIBA CORP

(72)Inventor : HARADA TOSHIHARU
TATEBAYASHI MAKOTO
KOZUKA MASAYUKI
HIROTA TERUTO
KAMIBAYASHI TATSU
TAMURA MASABUMI

(30)Priority
Priority number : 1999 436035 Priority date : 08.11.1999 Priority country : US

(54) STORAGE MEDIUM AND METHOD AND DEVICE FOR UPDATING REVOCATION INFORMATION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a storage medium or the like for excluding any access to contents in respect to illegal electronic equipment generated afterwards.
SOLUTION: A storage media (PM) 13 is provided with a controller 130 and two kinds of storage areas (a secret area 134 and a public area 131). The public area 131 is provided with a public R/W area 133 for storing digital contents and a public ROM-W area 132a for storing the identification information of electronic equipment being the object of the inhibition of any access to the digital contents as revocation information, and a public ROM area 132 for storing the identification information of the electronic equipment being the object of the inhibition of the update of the revocation information as master revocation information. When this storage medium is mounted on the electronic equipment having the identification information registered in the public ROM area 132, the controller 130 rejects the update of the revocation information by the electronic equipment.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－166996
（P2001－166996A）
(43)公開日　平成13年６月22日(2001.6.22)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０６Ｆ　12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｋ	
	３２０		３２０Ａ	
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ	
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ａ	

審査請求　未請求　請求項の数19　ＯＬ　（全 17 頁）　最終頁に続く

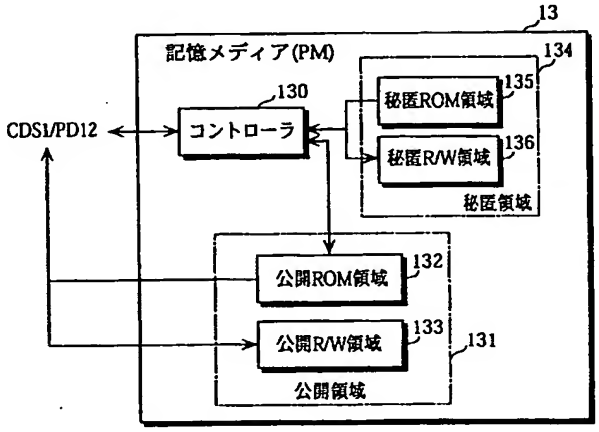
(21)出願番号　特願2000－252462(P2000－252462)
(22)出願日　平成12年８月23日(2000.8.23)
(31)優先権主張番号　０９／４３６０３５
(32)優先日　平成11年11月８日(1999.11.8)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　原田　俊治
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100090446
弁理士　中島　司朗　（外１名）

最終頁に続く

(54)【発明の名称】　記憶媒体、リポケーション情報更新方法及び装置

(57)【要約】
【課題】　後発的に発生した不正な電子機器に対しても、コンテンツへのアクセスを排除することが可能な記憶媒体等を提供する。
【解決手段】　記憶メディア（PM）１３は、コントローラ１３０と２種類の記憶領域（秘匿領域１３４及び公開領域１３１）とを有する。公開領域１３１は、デジタルコンテンツを記憶するための公開R/W領域１３３と、そのデジタルコンテンツへのアクセスを禁止する対象となる電子機器の識別情報をリポケーション情報として記憶するための公開ROM-W領域１３２ａと、そのリポケーション情報の更新を禁止する対象となる電子機器の識別情報をマスタリポケーション情報として記憶している公開ROM領域１３２とを備える。コントローラ１３０は、公開ROM領域１３２に登録された識別情報を有する電子機器に装着された場合には、その電子機器によるリポケーション情報の更新を拒否する。



1

【特許請求の範囲】

【請求項１】　電子機器に装着されて使用される記憶媒体であって、

デジタルコンテンツを記憶するためのコンテンツ記憶領域と、

前記コンテンツ記憶領域に記憶されたデジタルコンテンツへのアクセスを禁止する対象となる電子機器の識別情報に対応する情報をリボケーション情報として記憶するためのリボケーション情報記憶領域と、

前記リボケーション情報記憶領域に記憶されるリボケーション情報の更新を禁止する対象となる電子機器の識別情報に対応する情報をマスタリボケーション情報として記憶しているマスタリボケーション情報記憶領域とを備えることを特徴とする記憶媒体。

【請求項２】　前記記憶媒体は、さらに、

当該記憶媒体が装着された電子機器の識別情報が前記リボケーション情報記憶領域に記憶されたリボケーション情報に対応する識別情報に該当するか否かを判断し、該当しないと判断された場合にのみ、前記コンテンツ記憶領域に記憶されたデジタルコンテンツへの前記電子機器によるアクセスを許可するコンテンツ保護手段と、

前記電子機器の識別情報が前記マスタリボケーション情報記憶領域に記憶されたマスタリボケーション情報に対応する識別情報に該当するか否かを判断し、該当しないと判断された場合にのみ、前記電子機器からの指示に従って、前記リボケーション情報記憶領域に記憶されるリボケーション情報を更新するリボケーション情報更新手段とを備えることを特徴とする請求項１記載の記憶媒体。

【請求項３】　前記マスタリボケーション情報記憶領域は、予めマスタリボケーション情報が記憶されたＲＯＭであることを特徴とする請求項２記載の記憶媒体。

【請求項４】　前記記憶媒体は、さらに、

前記リボケーション情報更新手段によるリボケーション情報の更新の許否判断に先立って、前記電子機器と相互認証をし、相互認証に成功した場合にのみ前記電子機器と共有し合うことができる秘密鍵を生成する相互認証手段を備え、

前記リボケーション情報更新手段は、前記相互認証手段が生成した秘密鍵を用いて前記リボケーション情報を更新することを特徴とする請求項２記載の記憶媒体。

【請求項５】　前記リボケーション情報更新手段は、前記識別情報が前記マスタリボケーション情報に対応する識別情報に該当しないと判断した場合には、前記電子機器がリボケーション情報を更新するために必要となる秘密鍵を前記電子機器に送信することを特徴とする請求項２記載の記憶媒体。

【請求項６】　前記リボケーション情報記憶領域は、複数のグループに分類してリボケーション情報を記憶するための複数の記憶領域を有し、

2

前記リボケーション情報更新手段は、当該記憶媒体に装着された電子機器の識別情報が前記マスタリボケーション情報記憶領域に記憶されたマスタリボケーション情報に対応する識別情報に該当しないと判断し、かつ、前記電子機器の識別情報が前記リボケーション情報記憶領域に記憶されたリボケーション情報のうち前記電子機器が更新しようとしいるグループに属するリボケーション情報に対応する識別情報に該当しないと判断した場合に、前記グループに属するリボケーション情報だけを更新することを特徴とする請求項２記載の記憶媒体。

【請求項７】　前記リボケーション情報記憶領域は、前記デジタルコンテンツへのアクセスを禁止する対象となる電子機器の識別情報を鍵として特定の秘密鍵を暗号化して得られる情報をリボケーション情報として記憶し、

前記コンテンツ保護手段は、前記リボケーション情報記憶領域に記憶されたリボケーション情報を当該記憶媒体が装着された電子機器に送信し、それに対する前記電子機器からの返信情報が一定の規則性を有するか否か判断することによって、当該電子機器の識別情報が前記リボケーション情報記憶領域に記憶されたリボケーション情報に対応する識別情報に該当するか否かを判断し、

前記マスタリボケーション情報記憶領域は、前記リボケーション情報の更新を禁止する対象となる電子機器の識別情報を鍵として特定の秘密鍵を暗号化して得られる情報をマスタリボケーション情報として記憶し、

前記リボケーション情報更新手段は、前記マスタリボケーション情報記憶領域に記憶されたマスタリボケーション情報を当該記憶媒体が装着された電子機器に送信し、それに対する前記電子機器からの返信情報が一定の規則性を有するか否か判断することによって、前記電子機器の識別情報が前記マスタリボケーション情報記憶領域に記憶されたリボケーション情報に対応する識別情報に該当するか否かを判断するを備えることを特徴とする請求項２記載の記憶媒体。

【請求項８】　請求項１記載の記憶媒体のリボケーション情報を更新する方法であって、

記憶媒体が電子機器に装着されたことを検出する検出ステップと、

前記電子機器が有する第１の識別情報が前記記憶媒体のマスタリボケーション情報記憶領域に記憶されたマスタリボケーション情報に対応する識別情報に該当するか否かを判断する判断ステップと、

該当しないと判断された場合にのみ、前記リボケーション情報記憶領域に記憶されるリボケーション情報を更新する更新ステップとを含むことを特徴とするリボケーション情報更新方法。

【請求項９】　前記更新ステップでは、前記電子機器が有する第２の識別情報に対応する情報を新しいリボケーション情報として前記リボケーション情報記憶領域に記憶させることを特徴とする請求項８記載のリボケーショ

ン情報更新方法。

【請求項１０】　前記リボケーション情報更新方法は、さらに、

前記電子機器と前記記憶媒体とが相互認証をし、相互認証に成功した場合にのみ前記電子機器と前記記憶媒体とが共有し合うことができる秘密鍵を生成する相互認証ステップを含み、

前記更新ステップでは、前記相互認証ステップで生成された秘密鍵を用いて前記リボケーション情報を更新するを含むことを特徴とする請求項９記載のリボケーション情報更新方法。

【請求項１１】　前記更新ステップは、

前記第１の識別情報が前記マスタリボケーション情報に対応する識別情報に該当しないと判断した場合に、前記相互認証で共有された秘密鍵を用いて、前記第２の識別情報に対応する情報を新しいリボケーション情報として暗号化した後に、前記電子機器から前記記憶媒体に転送するサブステップと、

転送されてきた前記第２の識別情報に対応する情報を前記秘密鍵で復号化した後に、前記リボケーション情報記憶領域に記憶させるサブステップとを含むことを特徴とする請求項１０記載のリボケーション情報更新方法。

【請求項１２】　前記判断ステップは、さらに、前記第２の識別情報が前記リボケーション情報記憶領域に記憶されたリボケーション情報に該当するか否かを判断するサブステップを含み、

前記更新ステップでは、前記判断ステップにおいて、前記第１の識別情報が前記マスタリボケーション情報記憶領域に記憶されたマスタリボケーション情報に対応する識別情報に該当しないと判断され、かつ、前記第２の識別情報が前記リボケーション情報記憶領域に記憶されたリボケーション情報に該当しないと判断された場合に、前記第２の識別情報に対応する情報を新しいリボケーション情報として前記リボケーション情報記憶領域に記憶させることを特徴とする請求項９記載のリボケーション情報更新方法。

【請求項１３】　前記マスタリボケーション情報記憶領域は、前記リボケーション情報の更新を禁止する対象となる電子機器の識別情報を鍵として特定の秘密鍵を暗号化して得られる情報をマスタリボケーション情報として記憶し、

前記判断ステップでは、前記マスタリボケーション情報記憶領域に記憶されたマスタリボケーション情報を当該記憶媒体が装着された電子機器に送信し、それに対する前記電子機器からの返信情報が一定の規則性を有するか否か判断することによって、前記電子機器が有する第１の識別情報が前記記憶媒体のマスタリボケーション情報記憶領域に記憶されたマスタリボケーション情報に対応する識別情報に該当するか否かを判断することを特徴とする請求項９記載のリボケーション情報更新方法。

【請求項１４】　請求項１記載の記憶媒体のリボケーション情報を更新する装置であって、

前記記憶媒体のマスタリボケーション情報記憶領域に記憶されたマスタリボケーション情報に対応する識別情報に該当しない第１の識別情報を記憶している第１識別情報記憶手段と、

前記第１記憶情報記憶手段に記憶された第１の識別情報に対応する情報を用いて、前記記憶媒体から、前記記憶媒体に記憶されるリボケーション情報を更新する許可を取得する許可取得手段と、

取得した許可に従って前記記憶媒体に記憶されるリボケーション情報を更新する更新手段とを備えることを特徴とするリボケーション情報更新装置。

【請求項１５】　前記更新手段は、予め記憶している第２の識別情報に対応する情報を用いて前記リボケーション情報を更新することを特徴とする請求項１４記載のリボケーション情報更新装置。

【請求項１６】　前記リボケーション情報更新装置は、さらに、

前記記憶媒体による前記リボケーション情報の更新の許否判定に先立って、前記記憶媒体と相互認証をし、相互認証に成功した場合にのみ前記記憶媒体と共有し合うことができる秘密鍵を生成する相互認証手段を備え、

前記更新手段は、前記相互認証で共有された秘密鍵を用いて、前記リボケーション情報を更新することを特徴とする請求項１５記載のリボケーション情報更新装置。

【請求項１７】　前記更新手段は、前記相互認証で共有された秘密鍵を用いて、前記第２の識別情報に対応する情報を新しいリボケーション情報として暗号化した後に、前記電子機器から前記記憶媒体に転送することによって、前記リボケーション情報を更新することを特徴とする請求項１６記載のリボケーション情報更新装置。

【請求項１８】　前記リボケーション情報記憶領域は、複数のグループに分類してリボケーション情報を記憶するための複数の記憶領域を有し、

前記更新手段は、前記第２の識別情報に対応する１つのグループに属するリボケーション情報だけを更新することを特徴とする請求項１５記載のリボケーション情報更新装置。

【請求項１９】　前記マスタリボケーション情報記憶領域は、前記リボケーション情報の更新を禁止する対象となる電子機器の識別情報を鍵として特定の秘密鍵を暗号化して得られる情報をマスタリボケーション情報として記憶し、

前記許可取得手段は、前記記憶媒体から送信されてくるマスタリボケーション情報を受信し、前記第１の識別情報で復号化した後に、その復号結果と一定の規則性を有する情報を前記記憶媒体に返信することによって前記許可を取得することを特徴とする請求項１５記載のリボケーション情報更新装置。

5

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、デジタル化された文書、音声、画像、プログラムなどのデジタルコンテンツを格納しておくための記憶媒体、不当な電子機器によるデジタルコンテンツの記録や再生を抑止するのに用いられるリボケーション情報を更新する方法及び装置に関する。

【０００２】

【従来の技術】近年、デジタル技術やマイクロプロセッサ応用技術の発達に伴い、マルチメディア対応のパーソナルコンピュータ、セットトップボックス、プレーヤ、ゲーム機などの各種電子機器が開発されている。この種の電子機器は、記録メディアに格納された画像データや音楽データなど様々なデジタルコンテンツを再生できるほか、インターネット等を通じてデジタルコンテンツをダウンロードして使用することもできる。

【０００３】これらのデジタルコンテンツは、例えば、MPEG２、MP３といったデジタル符号化技術の採用により、品質を落とすことなくコピーしたり、ダウンロードすることができる。このため最近では、著作権保護の観点から、このようなデジタルコンテンツを不正使用から保護するための技術の必要性が叫ばれている。しかしながら、パーソナルコンピュータ、セットトップボックス、プレーヤなどの電子機器で用いられる記憶媒体は、別の電子機器に移動しても記録再生できるリバーシブルなものが多く、その仕様は基本的にオープンである。このため、コンテンツの移動／コピーを自由に行うことができるので、記憶媒体に記憶されたコンテンツを不正なコピー／移動から保護することは実際上困難である。

【０００４】そこでメモリカードのように記憶メディア部とコントローラが一体化された記憶媒体については、コントローラによるアクセス制御機能によって、秘匿された特定手続きでのみアクセスでき、ユーザからはアクセスできないアクセス不能領域（秘匿領域）を設け、そこにコピー制御情報、移動制御情報などの、コンテンツの使用に必要な重要な情報を格納しておくことで、コンテンツの保護を図ることが考えられる。

【０００５】この場合、パーソナルコンピュータ、セットトップボックス、プレーヤなどの電子機器と記憶媒体の間でコンテンツのコピー／移動を行う際には、それぞれが、著作権保護（コンテンツ保護）に関する仕組み（つまり所定のコンテンツ保護機能）を共有している正当なものであるかを相互認証し、正しいと認められた場合に相互に共有する鍵生成のアルゴリズムに従って鍵交換を行って個別に共通の認証鍵を取得し、その認証鍵をコンテンツキー（コンテンツを暗号化するキー）の暗号化／復号化またはコンテンツの暗号化／復号化に用いることも考えられる。

【０００６】

6

【発明が解決しようとする課題】ところが、上述のような著作権保護のための仕組み（例えば相互認証に必要な情報やプログラム等）は、電子機器の出荷段階で予め設定されていることから、機器の購入後に当該電子機器（上で動作するプログラム等）が改変されるといった攻撃によってコンテンツ保護の仕組みが無用のものになってしまった場合においては、もはや、相互認証だけではこの種の不正な電子機器を検出して排除することができず、著作権は侵害されてしまう。

【０００７】この対策として、いわゆるブラックリストとしてのリボケーション情報、即ち、記憶媒体に格納されているコンテンツへのアクセスを禁止する対象となる電子機器（の識別情報の一覧）を示すリボケーション情報を記憶媒体の特定記憶領域に予め登録しておき、このような記憶媒体が、リボケーション情報として登録された電子機器に装着して使用されようとした場合に、その電子機器の当該記憶媒体へのアクセスを禁止する、つまり、当該記憶媒体へのアクセス権を無効化することによってコンテンツの保護を図ることも考えられる。

【０００８】ところが、このような方策であっても、リボケーション情報自体は記憶媒体の出荷段階において書き換え不可能な記憶領域等に登録される必要があることから、当該記憶媒体の出荷後において、ある電子機器（上で動作するプログラム）の改変が行われた場合には、そのような不正な電子機器をリボケーション情報に追加登録することができないために、やはり、この種の電子機器による不正なアクセスを排除できない。

【０００９】そこで、本発明は、上記事情を考慮してなされたものであり、リボケーション情報を参照することによって不正な電子機器によるコンテンツへのアクセスを排除する機能を有する記憶媒体であって、後発的に発生した不正な電子機器に対しても、コンテンツへのアクセスを排除することが可能な記憶媒体、そのためのリボケーション情報更新方法及び装置を提供することを目的とする。

【００１０】

【課題を解決するための手段】上記目的を達成するために、電子機器に装着されて使用される記憶媒体であって、デジタルコンテンツを記憶するためのコンテンツ記憶領域と、前記コンテンツ記憶領域に記憶されたデジタルコンテンツへのアクセスを禁止する対象となる電子機器の識別情報に対応する情報をリボケーション情報として記憶するためのリボケーション情報記憶領域と、前記リボケーション情報記憶領域に記憶されるリボケーション情報の更新を禁止する対象となる電子機器の識別情報に対応する情報をマスタリボケーション情報として記憶しているマスタリボケーション情報記憶領域とを備えることを特徴とする。

【００１１】また、本発明に係るリボケーション情報更新方法は、上記記憶媒体のリボケーション情報を更新す

る方法であって、記憶媒体が電子機器に装着されたことを検出する検出ステップと、前記電子機器が有する第１の識別情報が前記記憶媒体のマスタリボケーション情報記憶領域に記憶されたマスタリボケーション情報に対応する識別情報に該当するか否かを判断する判断ステップと、該当しないと判断された場合にのみ、前記リボケーション情報記憶領域に記憶されるリボケーション情報を更新する更新ステップとを含むことを特徴とする。

【００１２】さらに、本発明に係るリボケーション情報更新装置は、上記記憶媒体のリボケーション情報を更新する装置であって、前記記憶媒体のマスタリボケーション情報記憶領域に記憶されたマスタリボケーション情報に対応する識別情報に該当しない第１の識別情報を記憶している第１識別情報記憶手段と、前記第１記憶情報記憶手段に記憶された第１の識別情報に対応する情報を用いて、前記記憶媒体から、前記記憶媒体に記憶されるリボケーション情報を更新する許可を取得する許可取得手段と、取得した許可に従って前記記憶媒体に記憶されるリボケーション情報を更新する更新手段とを備えることを特徴とする。

【００１３】つまり、記憶媒体の特定の記憶領域に、コンテンツへのアクセスを禁止すべき１つ以上の電子機器を特定するリボケーション情報と、当該リボケーション情報を更新することが特別に許可された電子機器を特定する（特別なリボケーション情報である）マスタリボケーション情報とを予め登録した構成とし、これによって、当該記憶媒体が、当該マスタリボケーション情報で表される電子機器に装着して使用された場合に、リボケーション情報の更新を許可する。

【００１４】具体的には、記憶メディア（PM）は、コントローラと２種類の記憶領域（秘匿領域及び公開領域）とを有する。公開領域は、デジタルコンテンツを記憶するための公開R/W領域と、そのデジタルコンテンツへのアクセスを禁止する対象となる電子機器の識別情報をリボケーション情報として記憶するための公開ROM-W領域と、そのリボケーション情報の更新を禁止する対象となる電子機器の識別情報をマスタリボケーション情報として記憶している公開ROM領域とを備える。コントローラは、公開ROM領域にマスタリボケーション情報として登録された識別情報を有する電子機器に装着された場合には、その電子機器によるリボケーション情報の更新を拒否する。

【００１５】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。図１は、本実施の形態における著作権保護システム１００の構成要素を示す図である。この著作権保護システム１００は、電子配信や記録媒体により流通されるデジタル著作物の著作権を保護するシステムであり、インターネットや放送等の通信網を介して音楽コンテンツを電子配信する自動販売機であるコンテンツ販売システム（CONTENT DISTRIBUTE SYSTEM（CDS））１と、音楽コンテンツを格納しておくための記憶メディア（PORTABLE MEDIA（PM））１３、PM１３に音楽コンテンツを記録したりPM１３に記録された音楽コンテンツを再生するための携帯型の記録再生装置（PORTABLE DEVICE（PD））１２と、音楽コンテンツを記録・再生・移動等によって管理をする装置であるコンテンツ利用管理システム（LICENSE COMPLIANT MODULE（LCM））２１から構成される。

【００１６】これらCDS１、PM１３及びPD１２は、上述したリボケーション情報を更新することによって、後発的に発生した不正な電子機器であっても、そのような電子機器によるデジタル著作物への不正なアクセスを排除することができる機能や構造を有している。図２は、CDS１の構成を示すブロック図である。ここで、ELECTRONIC MUSIC DISTRIBUTOR（EMD）４０は、音楽配信サーバや音楽放送局等であり、リボケーション情報発行機関（REVOCATION INFORMATION LICENSING ENTITY（RLE））４１は、不正な電子機器が新たに判明した場合等において、その電子機器の識別情報を含む新たなリボケーション情報を発行する機関（コンピュータ等）である。

【００１７】CDS１は、例えば、レコード店等に置かれる専用端末（KIOSK端末）等として実現されるものであり、EMD４０及びRLE４１と伝送路で接続され、セキュア・コンテンツ・サーバ（SECURE MUSIC SERVER（SMS））２、EMD_I/F（INTERFACE）部３、PD_I/F部５、メディア_I/F部６、秘匿領域ドライバ７、宿帳格納部８、ライセンス格納部９、音楽データ格納部１０、リボケーション情報受信部１４、ユーザ_I/F部１５、リボケーション情報格納部１６から構成され、以下の機能を有する。

【００１８】（１）コンテンツの記録（購入）機能
装着されたPM１３に、利用者が指定したコンテンツを記録（購入）する。
（２）リボケーション情報の更新機能
装着されたPM１３に、無効化すべき電子機器を示すリボケーション情報を記録し更新する。

【００１９】EMD_I/F部３は、複数のEMD４０と接続するための通信アダプタ等であり、PD_I/F部５は、PD１２と接続するUSB（UNIVERSAL SERIAL BUS）等であり、メディア_I/F部６は、PM１３を装着するためのPCMCIA用のカードスロット等であり、リボケーション情報受信部１４は、RLE４１から、登録すべき新たなリボケーション情報を受信する通信アダプタ等であり、ユーザ_I/F部１５は、LCDやスイッチ・ボタンキー等である。

【００２０】音楽データ格納部１０は、暗号化された音楽コンテンツを格納するためのフラッシュメモリ等であり、宿帳格納部８は、音楽データ格納部１０に格納された音楽コンテンツの属性情報等を格納するためのメモリ等であり、ライセンス格納部９は、音楽データ格納部１０に格納された暗号化音楽コンテンツを復号するための

9

鍵等を格納するためのメモリ等であり、リボケーション情報格納部１６は、RLE４１等から受信したリボケーション情報を一時的に格納しておくためのメモリ等である。

【００２１】秘匿領域ドライバ７は、ユーザには公開されていない秘匿された手順で宿帳格納部８等の後述する秘匿領域の記憶領域に対して、ユーザには公開されていない特定手順でアクセスする制御回路等であり、SMS２は、これら構成要素を制御することで上述の２つの機能を発揮する処理を実行するCPU等である。以下、CDS１の各構成要素の機能及びSMS２の制御内容を、上記（１）、（２）の機能毎に説明する。

【００２２】（１）　コンテンツの記録（購入）機能

CDS１におけるコンテンツ保護の方法は、コンテンツを記録すべきPM１３毎にその記憶メディアの識別情報（メディアID）を用いてコンテンツの暗号化／復号化を行うことを前提としている。CDS１は、複数のEMD４０（ここでは、EMD#１～#３）に対応した受信部#１～#３を有しており、当該受信部#１～#３を通してEMD４０が配信する暗号化コンテンツ（ここでは音楽コンテンツ）またはライセンス情報（利用条件、暗号化コンテンツ復号キーなど）を受信する。ここで各EMD４０が配信する暗号化コンテンツは、それぞれ独立の暗号方式や、音声圧縮符号化方式を用いて作成されている。受信部#１～#３は再生機能や課金機能を有していても良い。また、利用者は、課金機能を利用して、気に入ったコンテンツを購入することが可能である。

【００２３】SMS２は、利用者が購入した暗号化コンテンツをEMD_I/F部３を経由して受け取る。このとき、暗号化コンテンツ（即ち、各EMD４０毎に独立の暗号方式や音声圧縮方式で作成された暗号化コンテンツ）は、必要に応じて、EMD_I/F部３で復号され、CDS１において音声圧縮符号化方式や暗号方式への変換（再暗号化）が施される。

【００２４】SMS２は暗号化コンテンツを受け取ると、それを音楽データ格納部１０に格納し、暗号化コンテンツを復号するための鍵（暗号化コンテンツ復号キー）をライセンス格納部９に格納する。ここでSMS２は、配信された音楽コンテンツを利用者が試聴するために再生機能を有していても良く、この場合、SMS２が管理する音楽コンテンツをCDS１上で再生することができる。

【００２５】SMS２は、また、メディアI/F部６に装着可能なメモリカード等のPM１３に対して、音楽データ格納部に格納された暗号化コンテンツ（音楽コンテンツ）を当該I/F部６経由で出力する機能を有している。PM１３は、PD１２上にセットして用いることで、当該PM１３に記録された暗号化コンテンツ（音楽コンテンツ）をPD１２上で復号し再生することができる。SMS２からPM１３へのコンテンツの記録は、メディアI/F部６を通じて直接行われるか、またはPD１２を経由して行うことができる。また、このPM１３は、LCM２１にセットして用いることで、当該PM１３に記録された暗号化コンテンツ（音楽コンテンツ）を、LCM２１上で復号し再生したり、LCM２１上に暗号化コンテンツ（音楽コンテンツ）を移動させて保管することができる。

10

【００２６】（２）　リボケーション情報更新機能

リボケーション情報は、コンテンツ保護のためにPM１３の利用（PM１３へのコンテンツの記録、PM１３からのコンテンツの読み出しや再生など）を無効化すべき電子機器（PD、LCM）が判別可能な情報であり、PM１３に、出荷段階で予め登録されている。

【００２７】リボケーション情報更新機能は、この出荷段階で登録されたリボケーション情報を、必要に応じて（すなわち、新たに無効化すべき機器が発生した場合に）、特別に許可された電子機器（ここではCDS１）を通じて、新しいリボケーション情報に更新する機能である。CDS１は、RLE４１から、新しいリボケーション情報（以下、「新リボケーション情報」という。）を受け取るリボケーション情報受信部１４を有している。ここで、RLE４１とCDS１間を転送される新リボケーション情報は、例えば、RLE４１とCDS１間で予め共有されている暗号鍵を用いて暗号化することにより、転送途上の不当な改変行為からが防止されるものとする。

【００２８】SMS２は、RLE４１が発行する暗号化された新リボケーション情報をリボケーション情報受信部１４を通して受け取り、復号した後、リボケーション情報格納部１６に格納する。SMS２は、メディアI/F部６に、メモリカード等のPM１３が装着された場合に（メディア_I/F部６によって装着が検出された場合に）、リボケーション情報格納部１６に格納されている新リボケーション情報を当該メディアI/F部６経由で出力する機能を有している。SMS２からPM１３への新リボケーション情報の記録は、メディアI/F部６を通じて直接行われるか、またはPD１２を経由して行うことができる。

【００２９】次にリボケーション情報の種類について説明する。ここで述べるPM１３は、音楽コンテンツの記録用としてだけでなく、それ以外のアプリケーションシステム（例えば電子BOOKなど）の記録用としても用いることができる。このとき、各アプリケーションシステムに対応する電子機器の無効化（電子機器が有するアクセス権を無効化すること）を各アプリケーションシステム毎に実施したり管理したりできるようにするために、各アプリケーションシステム毎にリボケーション情報を発行し、各アプリケーションシステム毎に特別に許可された電子機器は、当該アプリケーションシステムに対応するリボケーション情報のみを更新できる。即ち、ここで述べるCDS１は、音楽コンテンツを扱う電子機器（PD、LCM）を対象とするリボケーション情報のみを更新できる。

【００３０】これにより、万一、CDS１のリボケーショ

ン更新機能が改変され悪用されることがあっても、他のアプリケーションシステムへ影響を及ぼすことはない（即ち、他のアプリケーションシステムにおけるリボケーション情報の不当な更新は防止できる）。また、CDS１のように、リボケーション情報の更新を特別に許可された電子機器についても、PM１３に登録された特別なリボケーション情報（以下、「マスタリボケーション情報」という。）によって、無効化できるようにしている。つまり、リボケーション情報を更新することが許可された特別な電子機器を示すマスタリボケーション情報が、不正にリボケーション情報を改変する電子機器を知るためのブラックリストとして、この著作権保護システム１００に導入されている。

【００３１】例えば、ある特定のCDS１のリボケーション更新機能が改変され悪用されることがあっても、そのような不正なCDS1の識別情報をマスタリボケーション情報として登録しておくことで、そのCDS1によるリボケーション情報へのアクセスを排除することができるので、リボケーション情報の不正な改ざんを防止することができる。

【００３２】なお、本実施例では、マスタリボケーション情報については、本発明の方法で更新することは考えないものとする。マスタリボケーション情報の更新は、新しいマスタリボケーション情報が登録された記憶媒体を発行し、古いマスタリボケーション情報が登録された記憶媒体から、この新しいマスタリボケーション情報が登録された記憶媒体に置き換えていくことによって実現するものとする。

【００３３】図２中のPD（記録再生装置）１２のブロック構成図

図３は、PM１３の構成を示す機能ブロック図である。PM１３は、コントローラ１３０と、公開領域１３１及び秘匿領域１３４からなる記憶メディア部とから構成される。秘匿領域１３４は、コントローラ１３０を通して非公開の手順（つまり秘匿された特定手続）でしかアクセスできない論理的な記憶領域であり、コンテンツ復号に必要な情報を記憶するのに用いられる。秘匿領域１３４は、秘密の定数（例えば後述するマスタメディア固有鍵KM-M等）が記憶される秘匿ROM領域１３５と、秘密の変数（例えば後述するライセンスする側から提供されるライセンス復号キーや、暗号化されたコンテンツ復号キー、メディア固有鍵KM-１等）が記憶される秘匿R/W（リード／ライト）領域１３６からなる。ここで暗号化されたコンテンツ復号キー（以下、単に、「暗号化コンテンツキー」という。）は、コンテンツCを復号するための（当該コンテンツCに固有の）コンテンツキーKCを、PM１３に固有のメディア固有鍵KM-１で暗号化することで取得されるものである。

【００３４】またマスタメディア固有鍵KM-Mや、メディア固有鍵KM-１は、各PM１３に固有であればよく、シリアル番号や製造番号（PM１３個々の製造番号、または製造ロット番号）、他様々な識別情報を用いることができる。なお、KM-MやKM-１を、前述のPM１３に固有な識別情報とライセンス復号キーから生成するようにしても構わない。物理的には、秘匿ROM領域１３５は、例えばROM（読み出し専用不揮発メモリ）上に確保され、秘匿R／W領域１３６は、例えばフラッシュメモリ（書換え可能な不揮発性メモリ）の特定領域に確保される。

【００３５】公開領域１３１は、秘匿領域以外の、通常の手順でアクセス可能な論理的な領域であり、読み出し専用の公開領域である公開ROM領域１３２と、書換え可能な公開領域である公開R／W領域１３３からなる。但し、公開ROM領域１３２には、図４に示されるように、非公開の手順で（つまり秘匿された特定手続）でのみ書き換えできる領域である公開ROM-W領域１３２ａを含むものとする。

【００３６】図４は、記憶メディア（PM）の公開ROM領域の構成と記憶内容を示す図である。物理的には、公開ROM領域１３２は、例えばROM上に確保され、公開R／W領域１３３、及び公開ROM-W領域１３２ａは、例えばフラッシュメモリ上に確保される。なお、この公開ROM領域１３２、公開ROM-W領域１３２ａ、公開R／W領域１３３は、先の秘匿ROM領域１３５が確保されるROM、秘匿R／W領域１３６が確保されるフラッシュメモリ上に、それぞれ確保されるようにしても構わない。

【００３７】公開ROM領域１３２のうち公開ROM-W領域１３２ａを除く領域（以下、単に、「公開ROM領域１３２」という。）には、マスタリボケーション情報（RL-M）が、PM１３の出荷段階で予め登録されている。また、公開ROM-W領域１３２ａには、（１つ以上の）リボケーション情報（RL-1、RL-2・・）が、PM１３の出荷段階で予め登録されている。リボケーション情報については、CDS１等のリボケーション情報更新機能の実行により、新リボケーション情報が、PM１３のコントローラ１３０を通して秘匿の手順で、この公開ROM-W領域１３２ａに登録（更新）される。なお、公開ROM領域１３２に、本発明の方法により更新することを必要としない別の（１つ以上の）リボケーション情報を予め登録していても構わない。

【００３８】本実施の形態において、マスタリボケーション情報、及び、（１つ以上の）リボケーション情報は、具体的には、無効化すべき電子機器の識別情報（６４ビットのデバイスID）のリストである。そこで、以下の説明では、「リボケーション情報」に代えて「リボケーションリストRL」なる用語を用いる。以下、マスタリボケーションリストをRL-M、（１つ以上の）リボケーション情報を、アプリケーションごとにRL-１，RL-２，…と記述し、その中でRL-１を音楽コンテンツの記録再生に対応する電子機器（PD、LCM等）の無効化に利用されるリボケーションリストとする。

13

【００３９】公開R／W領域１３３には、暗号化コンテンツ等が適宜記憶されている。この暗号化コンテンツは、コンテンツをコンテンツキーKCで暗号化することで取得されるものである。図５は、CDS1の論理的な記憶領域を示す図である。CDS１は、公開ROM領域１１２及び公開R／W領域１１３からなる公開領域１１１と非公開の手順でしかアクセスできない秘匿領域１１４との各記憶領域を有している。

【００４０】公開R／W領域１１３には、図２に示す音楽データ格納部１０が確保されている。公開ROM領域１１２には、公開ROM-W領域が含まれており、この公開ROM-W領域に、図２に示すリボケーション情報格納部１６が確保されている。（即ち、図２のSMS２は、RLE４１から受け取った暗号化された新リボケーション情報を復号し、秘匿の手順で、復号された新リボケーション情報をこの公開ROM-W領域に格納する。

【００４１】秘匿領域１１４には、識別情報（デバイスID）ID_CDSが予め記憶されている。秘匿領域１１４には、また各コンテンツ毎のコンテンツキーKCが適宜記憶されている。また、この秘匿領域１１４に、図２に示す宿帳格納部８が確保されている。ここでSMS２の管理下にある音楽データ格納部１０（公開R／W領域１１３）に保持されている全ての音楽コンテンツは、その識別情報であるコンテンツID（TID）等をその属性として持つ。この属性情報を宿帳と呼び（秘匿領域１１４内の）宿帳格納部８に格納される。

【００４２】CDS１は、それぞれのSMS２によって宿帳格納部８にアクセスするための秘匿された特定の手続きが行われた後、宿帳格納部８（を提供する秘匿領域１１４）からデータを読み取るための秘匿領域ドライバ７を有している。なお、この宿帳は本発明に直接関係しないため、その利用方法の詳細については説明を省略する。PD１２は公開のROM領域１２２及び公開R／W領域１２３からなる公開領域１２１と非公開の手順でしかアクセスできない秘匿領域１２４との各記憶領域を有している。秘匿領域１２４には、PD１２の識別情報ID_PDが予め固定記憶されている。秘匿領域１２４にはまた、各コンテンツ毎のコンテンツキーKCが適宜記憶されている。

【００４３】図６は、PD１２の構成を示すブロック図である。図７は、PD１２の論理的な記憶領域を示す図である。PD１２は、半導体プレーヤ等であり、ハードウェア的には、CPU１２ａ、RAM１２ｂ、ROM１２ｃ、フラッシュメモリ１２ｄ、外部機器I/F部１２ｅ、メディアI/F部１２ｆ、暗号化音楽コンテンツを復号等するための復調部１２ｇ、圧縮音楽コンテンツを伸長等するためのデコーダ部１２ｈ及びD/A変換部１２ｉから構成され、論理的な記憶領域として、図７に示されるように、公開領域１２１と秘匿領域１２４とを有する。

【００４４】図６に示されるように、PM１３は、PD１２のメディアI/F部１２ｆに装着して利用される。CDS１

14

は、PD１２を介してPM１３に読み書きする場合は、CDS１内のPD_I/F部５、PD１２内の外部機器I/F部１２ｅ、メディアI/F部１２ｆを経由して当該PM１３の秘匿領域１３４（図３参照）にアクセスする。メディアI/F部１２ｆは、PM１３の秘匿領域１３４にアクセスするための秘匿領域アクセス部（図示せず）を有している。PD１２内の公開R／W領域１２３及び秘匿領域１２４は、例えばフラッシュメモリ上に確保されている。また公開ROM領域１２２は、ROM１２C上に確保されている。このROM１２Cには、PM１３との間で相互認証を行うためのプログラムが書き込まれている。PD１２では、CPU１２ａの制御のもと、このプログラムに従ってPM１３との間の相互認証等の処理が実行される。

【００４５】図８は、LCM２１の構成を示すブロック図である。LCM２１は、例えば、パーソナルコンピュータを用いて実現され、リボケーション情報の更新機能を有さない点を除けば、基本的にCDS１と同様の構成、即ち、SMS２２、EMD_I/F部２３、PD_I/F部２５、メディア_I/F部２６、秘匿領域ドライバ２７、宿帳格納部２８、ライセンス格納部２９、音楽データ格納部３０、CD_I/F部３１及びユーザ_I/F部３５を備える。

【００４６】したがって、LCM２１は、CDS１と同様に、EMD４０から暗号化コンテンツを受け取り、LCM２１上に保管したり、LCM２１上に保管された暗号化コンテンツを、記憶媒体PM１３に記録したり、記憶媒体PM１３上の音楽コンテンツをLCM２１上に移動保管するための機能を有している。図９は、LCM２１の論理的な記憶領域を示す図である。PM１３、CDS１、PD１２と同様に、LCM２１は、公開のROM領域２１２及び公開R／W領域２１３からなる公開領域２１１と非公開の手順でしかアクセスできない秘匿領域２１４との各記憶領域を有している。秘匿領域２１４には、LCM２１の識別情報ID_LCMが予め固定記憶されている。秘匿領域２１４にはまた、各コンテンツ毎のコンテンツキーKCが適宜記憶されている。

【００４７】PM１３は、LCM２１のメディアI/F部２６に装着して利用される。LCM２１がPM１３へ読み書きする場合は、LCM２１内のメディアI/F部２６を経由して当該PM１３の秘匿領域１３４にアクセスする。メディアI/F部２６は、PM１３の秘匿領域１３４にアクセスするための秘匿領域アクセス部（図示せず）を有している。LCM２１内の公開R／W領域２１３及び秘匿領域２１４は、例えばフラッシュメモリ上に確保されている。また公開ROM領域２１２は、ROM上に確保されている。このROMにはPM１３との間で相互認証を行うためのプログラムが書き込まれている。LCM２１では、CPU（図示せず）の制御のもと、このプログラムに従ってPM１３との間の相互認証等の処理が実行される。

【００４８】次に、本実施の形態における著作権保護システム１００の動作について、利用者が、PM１３を、CDS１に挿入し、あるEMD４０で配信された音楽コンテンツ

15

を、PM１３に記録（購入）する処理を選択した場合に、RLE（RLE４１）が発行し、CDS１によって既に保持されている新リボケーション情報が、当該音楽コンテンツとともに、PM１３に記録されるときの動作を例に、説明する。

【００４９】図１０及び図１１は、それぞれ、そのようなケースにおけるCDS１とPM１３間での通信と処理の流れにおける前半及び後半を示す図である。音楽コンテンツの購入指示が例えばCDS１のユーザインターフェース（I/F部）１５を介してなされ、かつ、PM１３がCDS１のメディアI/F部６に装着されたことが相互で検出された後に、CDS１のメディアI/F部とPM１３のコントローラ１３０との間で周知の相互認証（AKE（AUTHENTICATION AND KEY EXCHANGE）-M（MASTER））が行われる（ステップＳ１０１）。この相互認証AKE-Mは、例えばCDS１とPM１３の間で、次のように行われる。

【００５０】まず、CDS１からPM１３を認証する。ここで（リボケーションの更新を許可された特別の）CDS１は認証鍵K１-Mを保持しており、PM１３は、同じ認証鍵K１-Mを保持している（図示していないがいずれも秘匿ROM領域の保持されている）。CDS１は乱数R１を発生してPM１３に送る。PM１３は、CDS１で発生された乱数R１を受け取ると、それを認証鍵K１-Mで暗号化して、その暗号化された乱数（K１-M［R１］と表す）をCDS１に返す。CDS１では、認証鍵K１-Mを用いて、K１-M［R１］を復号し、復号結果が先に発生した乱数R１に等しければ、PM１３は正しい相手であると判定する。

【００５１】その後、上記と同じことをPM１３からCDS１に対して行うことで、相互認証を行う。この場合、CDS１、PM１３はそれぞれ認証鍵K２-Mを保持し、CDS１がPM１３で発生した乱数R２をK２-Mで暗号化してそれをPM１３でK２-Mを用いて復号し、先に発生した乱数R２に等しいかを確認する。ここで、認証鍵K１-M、K２-Mは、リボケーションの更新を許可された特別の電子機器（ここではCDS１）にのみ与えることにより、一般の電子機器（LCM２１など）による認証処理AKE-Mを行うことを防止することができる。

【００５２】以上の相互認証AKE-M（Ｓ１０１）により、CDS１及びPM１３が双方で正当な相手であることが確認されたとき、CDS１のメディアI/F部とPM１３のコントローラ１３０との間でキー交換が行われ、同一のセッション鍵（KY１）が共有される。このセッション鍵KY１は、例えば、上記で相互に発生しあった乱数R１とR２の排他的論理和値を、CDS１及びPM１３が予め共有している秘密の鍵生成アルゴリズムに、入力した際の出力値として求められ、従って、セッション鍵KY１は毎回変わる時変キーである。

【００５３】CDS１のメディアI/F部６は、秘匿領域１１４に秘匿（記憶）されている自身のマスタ識別情報ID-Mを読み出して当該ID-Mをセッション鍵KY１で暗号化し、

16

その暗号化されたID-M（=KY１[ID-M]）をメディアI/F部６からPM１３に送る（ステップＳ１０２）。PM１３のコントローラ１３０は、CDS１側からのKY１[ID-M]を、先のキー交換で取得したセッション鍵（KY１）で復号し、ID-Mを得る（ステップＳ１０３）。

【００５４】次にPM１３のコントローラ１３０は、復号したCDS１のマスタ識別情報ID-Mにより、公開ROM１３２内のマスタリボケーションリストRL-Mを参照し、当該ID-Mに一致する識別情報が登録されているか否かにより、CDS１によるPM１３の利用を無効化するか否かを判定する（ステップＳ１０４）。もし、ID-Mに一致する識別情報がマスタリボケーションリストRL-Mに登録されている場合には、コントローラ１３０は該当するCDS１によるPM１３の利用を無効化（リボケート）すべきものと判定し、以降の処理を停止する。

【００５５】これに対し、ID-Mに一致する識別情報がマスタリボケーションリストRL-Mに登録されていない場合は、コントローラ１３０は該当するCDS１によるPM１３の利用（リボケーション情報の更新）が許可されているものと判定し、秘匿ROM領域１３５に格納されている秘匿されているマスタメディア固有鍵KM-Mを読み出し出力する（ステップＳ１０５）。そしてコントローラ１３０は、CDS１のメディアI/Fの間で（当該CDS１のメディアI/F部６を介して）キー交換を行い、同一のセッション鍵KY２を共有した上で、上記読み出したマスタメディア固有鍵KM-Mをセッション鍵（KY２）で暗号化し、その暗号化されたKM-M（=KY２[KM-M]）をCDS１に送る（ステップＳ１０６）。ここで、セッション鍵KY２は、例えば、先のセッション鍵KY１を、CDS１及びPM１３が予め共有している秘密の鍵生成アルゴリズムに、入力した際の出力値として求められる。

【００５６】CDS１のメディアI/F部６は、PM１３側からのKY２[KM-M]を、先のキー交換で取得したセッション鍵（KY２）で復号し、マスタメディア固有鍵KM-Mを得る（ステップＳ１０７）。次にCDS１のメディアI/F部６は、公開ROM-W領域に格納されている新リボケーション情報RL-１、及び、メディアI/F部６で生成される新しいメディア固有鍵KM-１Nを取得したマスタメディア固有鍵KM-Mにより暗号化し、その暗号化されたKM-M[RL-M]及びKM-M[KM-１N]をPM１３に送る（ステップＳ１０８）。

【００５７】ここで、メディア固有鍵KM-１Nは、例えば、先のセッション鍵KY２を、CDS１が秘密に保持する鍵生成アルゴリズム入力したときに得られる出力値として生成されるものとする。PM１３のコントローラ１３０は、CDS１側からのKM-M[RL-M]及びKM-M[KM-１N]を、秘匿ROM領域１３５に格納されたKM-Mを用いて復号し、RL-M、KM-１Nを得る（ステップＳ１０９）。

【００５８】次に、CDS１のメディアI/F部とPM１３のコントローラ１３０との間で上述した相互認証（AKE-M）と同様の相互認証（AKE-１）が行われる（ステップＳ１

17

１０）。すなわち、まずは、CDS１からPM１３を認証する。ここでCDS１は認証鍵K１-１を保持しており、PM１３は、同じ認証鍵K１-１を保持している（図示していないがいずれも秘匿ROM領域の保持されている）。CDS１は乱数R３を発生してPM１３に送る。PM１３は、CDS１で発生された乱数R３を受け取ると、それを認証鍵K１-１で暗号化して、その暗号化された乱数（K１-１［R３］と表す）をCDS１に返す。CDS１では、認証鍵K１-１を用いて、K１-１［R３］を復号し、復号結果が先に発生した乱数R３に等しければ、PM１３は正しい相手であると判定する。

【００５９】その後、上記と同じことをPM１３からCDS１に対して行うことで、相互認証を行う。この場合、CDS１、PM１３はそれぞれ認証鍵K２-１を保持し、CDS１がPM１３で発生した乱数R２４をK２-１で暗号化してそれをPM１３でK２-１で復号し、先に発生した乱数R４に等しいかを確認する。ここで、認証鍵K１-１、K２-１は、音楽コンテンツの利用を許可された電子機器（ここではPD１２、LCM２１）にのみ与えることにより、他のアプリケーションシステムに対応する電子機器による認証処理AKE-１を行うことを防止することができる。

【００６０】以上の相互認証AKE-１（S１１０）により、CDS１及びPM１３が双方で正当な相手であることが確認されたとき、CDS１のメディアI/F部とPM１３のコントローラ１３０との間でキー交換が行われ、同一のセッション鍵（KX１）が共有される。このセッション鍵KX１は、例えば、上記で相互に発生しあった乱数R３とR４の排他的論理和値を、CDS１及びPM１３が予め共有している秘密の鍵生成アルゴリズムに、入力した際の出力値として求められ、従って、セッション鍵KX１は毎回変わる時変キーである。

【００６１】CDS１のメディアI/F部６は、秘匿領域１１４に秘匿（記憶）されている自身の識別情報ID-１を読み出して当該ID-１をセッション鍵KX１で暗号化し、その暗号化されたID-１（=KX１[ID-１]）をメディアI/F部６からPM１３に送る（ステップS１１１）。PM１３のコントローラ１３０は、CDS１側からのKX１[ID-１]を、先のキー交換で取得したセッション鍵（KX１）で復号し、ID-１を得る（ステップS１１２）。

【００６２】次にPM１３のコントローラ１３０は、復号したCDS１の識別情報ID-１により、公開ROM１３２内のリボケーションリストRL-１を参照し、当該ID-１に一致する識別情報が登録されているか否かにより、CDS１によるPM１３の利用を無効化するか否かを判定する（ステップS１１３）。もし、ID-１に一致する識別情報がリボケーションリストRL-１に登録されている場合には、コントローラ１３０は該当するCDS１によるPM１３の利用を無効化（リボケート）すべきものと判定し、以降の処理を停止する。

【００６３】これに対し、ID-１に一致する識別情報が

18

リボケーションリストRL-１に登録されていない場合は、コントローラ１３０は該当するCDS１によるPM１３の利用（コンテンツの記録）が許可されているものと判定し、ステップS１０９で得た新リボケーション情報RL-１N、新しいメディア固有鍵KM-１Nによって、RL-１、KM-１をそれぞれ更新する（ステップS１１４）。

【００６４】その後、図１１に示されるように、CDS１のメディアI/Fは、PM１３のコントローラ１３０の間で（当該CDS１のメディアI/F部６を介して）キー交換を行い、同一のセッション鍵KX２を共有した上で、CDS１のメディアI/F部６は、秘匿領域１１４に秘匿（記憶）されている自身の識別情報ID-１を読み出して当該ID-１をセッション鍵KX２で暗号化し、その暗号化されたID-１（=KX２[ID-１]）をメディアI/F部６からPM１３に送る（ステップS１１５）。ここで、セッション鍵KX２は、例えば、先のセッション鍵KX１を、CDS１及びPM１３が予め共有している秘密の鍵生成アルゴリズムに、入力した際の出力値として求められる。

【００６５】PM１３のコントローラ１３０は、CDS１側からのKX２[ID-１]を、先のキー交換で取得したセッション鍵（KX２）で復号し、ID-１を得る（ステップS１１６）。次にPM１３のコントローラ１３０は、復号したCDS１の識別情報ID-１により、公開ROM-W領域内の新リボケーションリストRL-１Nを参照し、当該ID-１に一致する識別情報が登録されているか否かにより、CDS１によるPM１３の利用を無効化するか否かを判定する（ステップS１１７）。

【００６６】もし、ID-Mに一致する識別情報がリボケーションリストRL-１Nに登録されている場合には、コントローラ１３０は該当するCDS１によるPM１３の利用を無効化（リボケート）すべきものと判定し、以降の処理を停止する。これに対し、ID-１に一致する識別情報がリボケーションリストRL-１Nに登録されていない場合は、コントローラ１３０は該当するCDS１によるPM１３の利用（コンテンツの記録）が許可されているものと判定し、秘匿ROM領域１３５に格納されている秘匿されているメディア固有鍵KM-１Nを読み出し出力する（ステップS１１８）。そしてコントローラ１３０は、CDS１のメディアI/Fの間で（当該CDS１のメディアI/F部６を介して）キー交換を行い、同一のセッション鍵KX３を共有した上で、上記読み出したメディア固有鍵KM-１Nをセッション鍵（KX３）で暗号化し、その暗号化されたKM-１N（=KX３[KM-１N]）をCDS１に送る（ステップS１１９）。ここで、セッション鍵KX３は、例えば、先のセッション鍵KX２を、CDS１及びPM１３が予め共有している秘密の鍵生成アルゴリズムに、入力した際の出力値として求められる。

【００６７】CDS１のメディアI/F部６は、PM１３側からのKX３[KM-１N]を、先のキー交換で取得したセッション鍵（KX３）で復号し、メディア固有鍵KM-１Nを得る（ス

19

テップＳ１２０）。次にCDS１のメディアI/F部６は、秘匿領域１１４に秘匿されているコンテンツキーKCを取得したメディア固有鍵KM-１Nにより暗号化し、暗号化されたKM-１N[KC]　をPM１３の秘匿R/W領域に送る（ステップＳ１２１）。

【００６８】また、CDS１のメディアI/F部６は、公開R/W領域１１３に格納されている暗号化コンテンツKC[C]を、PM１３の公開R/W領域に送る（ステップＳ１２２）。このように、本実施の形態では、マスタリボケーションリストRL-Mに従って無効化（リボケート）されたならば渡ることのない（暗号化された）マスタメディア固有鍵KM-Mを当該PM１３からCDS１が受け取り、そのCDS１の公開ROM領域１１４に格納されている新リボケーション情報RL-１、及び、メディア固有鍵KM-１Nを当該マスタメディア固有鍵KM-Mにより暗号化し、PM１３に送るようにしている。

【００６９】このため、マスタリボケーションリストRL-Mで指定される無効化対象CDS（PM１３のリボケーション情報を更新しようとする電子機器）を確実に無効化（排除）できる。さらにリボケーションリストRL-１に従って無効化（リボケート）されたならば、PM１３において、新リボケーション情報RL-１及びメディア固有鍵KM-１Nへの更新を行わない様にしている。さらに、新リボケーションリストRL-１Nに従って無効化（リボケート）されたならば渡ることのない（暗号化された）メディア固有鍵KM-１を当該PM１３からCDS１が受け取り、そのCDS１の秘匿領域１１４に格納されているコンテンツキーKCを当該メディア固有鍵KM-１Nにより暗号化し、PM１３に送るようにしている。このため、新リボケーションリストRL-１Nで指定される無効化対象CDS１（PM１３を利用しようとする電子機器）を確実に無効化（排除）できる。

【００７０】次に、PM１３に格納された暗号化コンテンツをPD１２上で復号して再生する場合の動作について、説明する。なお、以下の説明では、PD１２上で復号して再生する場合を例に説明するが、LCM２１上で復号して再生する場合も全く同じ手順で行われる。図１２は、そのようなケースにおけるPM１３とPD１２間での通信と処理の流れを示す図である。

【００７１】まず、再生指示が例えばPD１２に対してなされ、かつPM１３がPD１２のメディアI/F部１２ｆに装着された段階で、PD１２のCPU１２ａとPM１３のコントローラ１３０との間で（前記S１１０と同様の）相互認証AKE-１が行われる（ステップＳ２０１）。そして、この相互認証（S２０１）によりPD１２及びPM１３の双方で正当な相手であることが確認されたとき、PD１２のCPU１２ａとPM１３のコントローラ１３０との間でキー交換が行われ同一のセッション鍵（KX４）が共有される。

【００７２】PD１２のCPU１２ａは、秘匿領域１２４に秘匿されている自身の識別情報ID-PDを読み出して当該ID-PDをセッション鍵（KX４）で暗号化し、その暗号化されたID-PD（=KX４[ID-PD]）をメディアI/F部１２ｆからPM１３に送る（ステップＳ２０２）。PM１３のコントローラ１３０は、PD１２側からおｎKX４[ID-PD]を、先のキー交換で取得したセッション鍵（KX４）で復号し、ID-PDを得る（ステップＳ２０３）。

20

【００７３】PM１３のコントローラ１３０は、復号したPD１２の識別情報ID-PDにより公開ROM-W領域内のリボケーションリストRL-１Nを参照し、当該ID-PDに一致する識別情報が登録されているか否かにより、PD１２によるPM１３の利用を無効化するか否かを判定する（ステップＳ２０４）。もし、ID-PDに一致する識別情報がリボケーションリストRL-１Nに登録されている場合には、コントローラ１３０は該当するPD１２によるPM１３の利用を無効化（リボケート）すべきものと判定し、以降の処理を停止する。

【００７４】これに対し、ID-PDに一致する識別情報がリボケーションリストRL-１Nに登録されていない場合は、コントローラ１３０は該当するPD１２によるPM１３の利用が許可されているものと判定し、秘匿R/W領域１３６に秘匿されているメディア固有鍵KM-１Nを読み出し出力する（ステップＳ２０５）。そしてコントローラ１３０は、PD１２のCPU１２ａとの間で（当該PD１２NOメディアI/F部１２ｆを介して）キー交換を行い、同一のセッション鍵（KX５）を共有した上で、上記読み出したメディア固有鍵（KX５）で暗号化し、その暗号化されたKM-１N（=KX５[KM-１N]）をPD１２に送る（ステップＳ２０６）。ここで、セッション鍵KX５は、例えば、先のセッション鍵KX４を、PD１２及びPM１３が予め共有している秘密の鍵生成アルゴリズムに、入力した際の出力値として求められる。

【００７５】PD１２のCPU１２ａは、PM１３側からのKX５[KM-１N]を、先のキー交換で取得したセッション鍵（KX５）で復号し、メディア固有鍵KM-１Nを得る（ステップＳ２０７）。次に、PD１２のCPU１２ａは、PM１３の秘匿R/W領域１３６に記憶されている暗号化コンテンツキーKC（=KM-１N[KC]）を読み込んで、ステップＳ２０７で取得したメディア固有鍵KM-１Nにより復号する（ステップＳ２０８）。次に、PD１２のCPU１２ａは、PM１３の公開R/W領域１３３に記憶されている暗号化コンテンツC（=KC[C]）を読み込んで、ステップＳ２０８で取得したコンテンツキーKｃにより復号して再生する（ステップＳ２０８９）。

【００７６】このように、本実施の形態では、リボケーションリストRL-１Nに従って、無効化（リボケート）されたならばPM１３から渡されることのない（暗号化された）メディア固有鍵KM-１Nを当該PM１３からPD１２が受け取り、当該PM１３の秘匿R/W領域に秘匿されている暗号化コンテンツキー（KM-１N[KC]）をそのメディア固有鍵KM-１Nにより復号し、PD１２での暗号化コンテンツの

復号に利用するようにしている。このため、新リボケーションリストRL-1Nで指定される無効化対象PD（PM１３を利用しようとする電子機器）を確実に無効化できる。

【００７７】以上、本発明に係る著作権保護システム１００について、実施の形態に基づいて説明したが、本発明は、この実施の形態に限られないことは勿論である。例えば、本実施の形態では、著作権保護の対象となるデジタル著作物は、音楽コンテンツであったが、映画やゲームソフト等のデータであってもよい。また、本実施の形態では、CDS１とPM１３の間、PD１２とPM１３の間で、秘匿領域に秘匿されている情報、または秘匿領域に秘匿すべき情報の授受を行う際に、当該情報をセッション鍵（KYI、KXI）により暗号化するものとしたが、暗号化は必ずしも必要ではない。但し、コンテンツ保護をより確実なものにするためには、セッション鍵による暗号化を行うことが望ましい。

【００７８】また、本実施の形態では、マスタリボケーションリストRL-M、及びリボケーションリストRL-１,RL-１Nが公開ROM領域１３２（あるいは公開ROM-W領域）に登録されているものとして説明したが、リボケーションリストが改竄されない領域であれば良く、例えば秘匿された特定の手続きでしかアクセスできない秘匿領域１３４に登録されるようにしてもよい。

【００７９】また、本実施の形態では、暗号化コンテンツキー（KM-１N[KC]）は、秘匿R/W領域１３６に格納されるものとして説明したが、公開R/W領域１３３に格納されるようにしてもよい。また、本実施の形態では、電子機器の識別情報は、電子機器から記憶媒体に転送されたが、本発明は、そのような転送方向に限定されるものではなく、逆の転送方向であってもよい。

【００８０】例えば、記憶媒体は、リボケーション情報として、コンテンツへのアクセスを許可する電子機器については、所定の第１鍵K1をその電子機器の識別情報IDで暗号化して得られる値E(ID,K1)を記憶しておき、一方、コンテンツへのアクセスを禁止する電子機器については、所定の第２鍵K2をその電子機器の識別情報IDで暗号化して得られる値E(ID,K2)を記憶しておく。

【００８１】そして、記憶媒体が電子機器に装着されると、まず、記憶媒体は、上述のようなリボケーション情報Eと乱数Rを電子機器に送信する。それらE及びRを受け取った電子機器は、リボケーション情報Eを自分の識別情報IDで復号することによって、無効化されていない場合には、第１の鍵K1を取得し、一方、無効化されている場合には、第２の鍵K2を取得する。そして、取得した鍵K（K1又はK2）を乱数Rで暗号化し、得られた値E(K,R)を記憶媒体に返信する。

【００８２】記憶媒体は、受け取った値E(K,R)を復号し、得られた乱数R'と、電子機器に送信しておいた乱数Rとを比較し、一致する場合にのみ、コンテンツへのアクセスを許可すればよい。マスタリボケーション情報についても、同様の記憶内容と手順にすることで、電子機器の識別情報の転送方向を反転させることができる。

【００８３】

【発明の効果】以上の説明から明らかなように、電子機器に装着されて使用される記憶媒体であって、デジタルコンテンツを記憶するためのコンテンツ記憶領域と、前記コンテンツ記憶領域に記憶されたデジタルコンテンツへのアクセスを禁止する対象となる電子機器の識別情報に対応する情報をリボケーション情報として記憶するためのリボケーション情報記憶領域と、前記リボケーション情報記憶領域に記憶されるリボケーション情報の更新を禁止する対象となる電子機器の識別情報に対応する情報をマスタリボケーション情報として記憶しているマスタリボケーション情報記憶領域とを備えることを特徴とする。

【００８４】これによって、権限なくリボケーション情報を更新しようとする不正な電子機器の識別情報に対応する情報については、その記憶媒体のマスタリボケーション情報記憶領域に予め登録しておくことができるので、この情報を参照することで、リボケーション情報にアクセスしようとした電子機器が正当な電子機器であるか不正な電子機器であるかを知ることができる。

【００８５】したがって、リボケーション情報は、安全性が保証された書き換え可能な記憶領域に保管されるので、後発的に不正な電子機器が出現しても、その電子機器の識別情報に対応する情報をリボケーション情報記憶領域に追加登録することで、それ以降におけるデジタル著作物への不正なアクセスが排除される。ここで、前記記憶媒体は、さらに、当該記憶媒体が装着された電子機器の識別情報が前記リボケーション情報記憶領域に記憶されたリボケーション情報に対応する識別情報に該当するか否かを判断し、該当しないと判断された場合にのみ、前記コンテンツ記憶領域に記憶されたデジタルコンテンツへの前記電子機器によるアクセスを許可するコンテンツ保護手段と、前記電子機器の識別情報が前記マスタリボケーション情報記憶領域に記憶されたマスタリボケーション情報に対応する識別情報に該当するか否かを判断し、該当しないと判断された場合にのみ、前記電子機器からの指示に従って、前記リボケーション情報記憶領域に記憶されるリボケーション情報を更新するリボケーション情報更新手段とを備えてもよい。

【００８６】これによって、マスタリボケーション情報記憶領域に登録されていない識別情報を有する電子機器だけが、その記憶媒体のリボケーション情報を更新することが許可されるので、不正な電子機器によるリボケーション情報の改ざんが防止される。また、前記マスタリボケーション情報記憶領域は、予めマスタリボケーション情報が記憶されたＲＯＭとしてもよい。これによって、記憶媒体が出荷された後においてマスタリボケーション情報自体を改ざんする、という攻撃に備えることが

できる。

【００８７】また、前記記憶媒体は、さらに、前記リボケーション情報更新手段によるリボケーション情報の更新の許否判断に先立って、前記電子機器と相互認証をし、相互認証に成功した場合にのみ前記電子機器と共有し合うことができる秘密鍵を生成する相互認証手段を備え、前記リボケーション情報更新手段は、前記相互認証手段が生成した秘密鍵を用いて前記リボケーション情報を更新してもよい。

【００８８】これによって、リボケーション情報を更新する権限に関わる極めて重要な識別情報は、秘匿化された状態で記憶媒体と電子機器間で転送されるので、リボケーション情報の改ざんに対する防御が強化される。また、前記リボケーション情報更新手段は、前記識別情報が前記マスタリボケーション情報に対応する識別情報に該当しないと判断した場合には、前記電子機器がリボケーション情報を更新するために必要となる秘密鍵を前記電子機器に送信してもよい。

【００８９】これによって、リボケーション情報の更新権限の有無に関する判断結果が秘匿化され、それら装置間を盗聴する不正行為に備えることができる。また、前記リボケーション情報記憶領域は、複数のグループに分類してリボケーション情報を記憶するための複数の記憶領域を有し、前記リボケーション情報更新手段は、当該記憶媒体に装着された電子機器の識別情報が前記マスタリボケーション情報記憶領域に記憶されたマスタリボケーション情報に対応する識別情報に該当しないと判断し、かつ、前記電子機器の識別情報が前記リボケーション情報記憶領域に記憶されたリボケーション情報のうち前記電子機器が更新しようとしいるグループに属するリボケーション情報に対応する識別情報に該当しないと判断した場合に、前記グループに属するリボケーション情報だけを更新してもよい。

【００９０】これによって、リボケーション情報が不正に改ざんされるという攻撃を受けた場合であっても、他のアプリケーションシステムはその影響を受けないので、被害は最小限に抑えられる。

【図面の簡単な説明】

【図１】本発明の実施の形態における著作権保護システムの全体構成を示す概観図である。

【図２】コンテンツ販売システム（CONTENT DISTRIBUTE SYSTEM（CDS））の構成を示すブロック図である。

【図３】記憶メディア（PORTABLE MEDIA（PM））の構成を示すブロック図である。

【図４】記憶メディア（PM）の公開ROM領域の構成と記憶内容を示す図である。

【図５】CDSの論理的な記憶領域を示す図である。

【図６】記録再生装置（PORTABLE DEVICE（PD））の構成を示すブロック図である。

【図７】PDの論理的な記憶領域を示す図である。

【図８】コンテンツ利用管理システム（LICENSE COMPLIANT MODULE（LCM））の構成を示すブロック図である。

【図９】LCMの論理的な記憶領域を示す図である。

【図１０】CDSとPM間での通信と処理の流れにおける前半を示す図である。

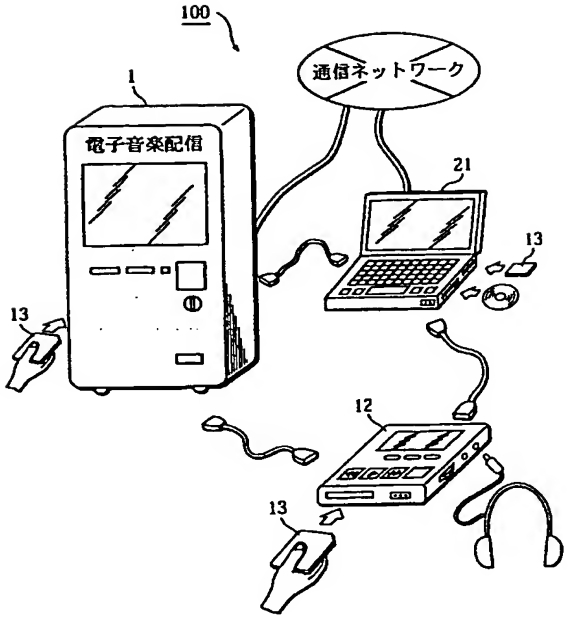
【図１１】CDSとPM間での通信と処理の流れにおける後半を示す図である。

【図１２】PMとPD間での通信と処理の流れを示す図である。

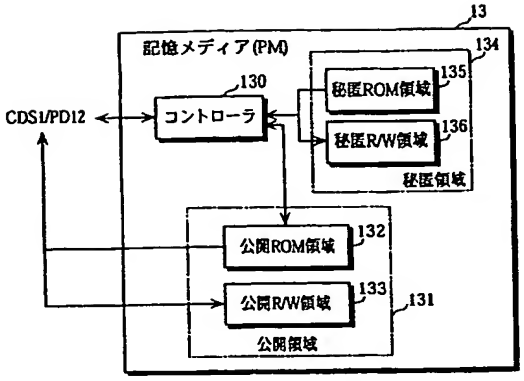
【符号の説明】

１　コンテンツ販売システム（CDS）
２、２２　セキュア・コンテンツ・サーバ（SMS）
３、２３　EMD_I/F部
５、２５　PD_I/F部
６、２６　メディア_I/F部
７、２７　秘匿領域ドライバ
８、２８　宿帳格納部
９、２９　ライセンス格納部
１０、３０　音楽データ格納部
１２　記録再生装置（PD）
１３　記憶メディア（PM）
１４　リボケーション情報受信部
１５、３５　ユーザ_I/F部
１６　リボケーション情報格納部
２１　コンテンツ利用管理システム（LCM）
３１　CD_I/F部部
１００　著作権保護システム
１１１、１２１、１３１、２１１　公開領域
１１２、１２２、１３２、２１２　公開ROM領域
１３２ａ　公開ROM-W領域
１１３、１２３、１３３、２１３　公開R/W領域
１１４、１２４、１３４、２１４　秘匿領域
１３０　コントローラ
１３４　秘匿領域
１３５　秘匿ROM領域
１３６　秘匿R/W領域

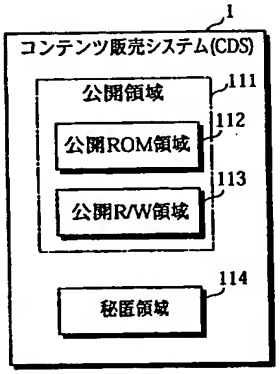
【図１】


100
通信ネットワーク
1
電子音楽配信
21
13
13
12
13

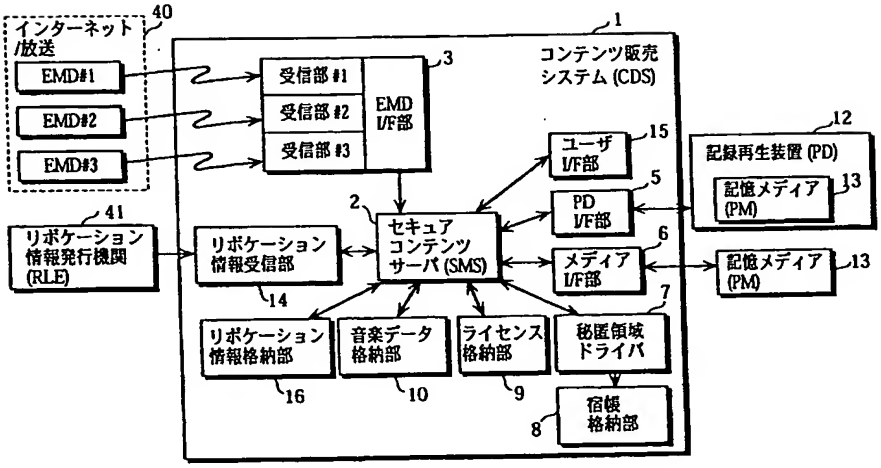
【図３】


13
記憶メディア(PM)
134
130
秘匿ROM領域
135
CDS1/PD12
コントローラ
秘匿R/W領域
136
秘匿領域
公開ROM領域
132
公開R/W領域
133
131
公開領域

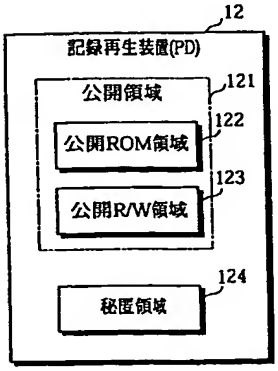
【図５】


1
コンテンツ販売システム(CDS)
公開領域
111
公開ROM領域
112
113
公開R/W領域
秘匿領域
114

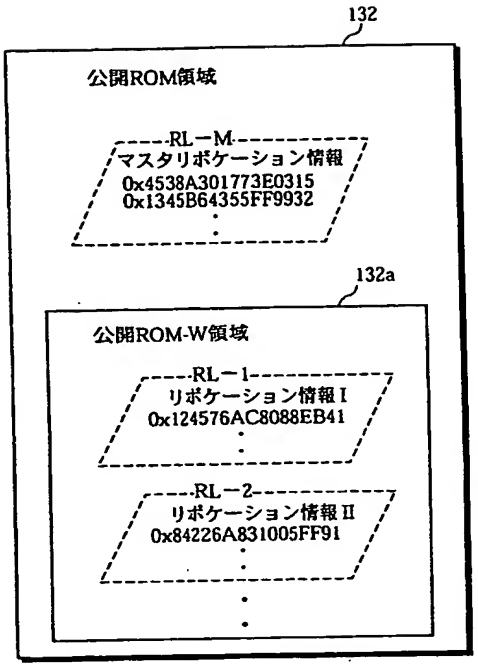
【図２】


インターネット/放送
40
EMD#1
EMD#2
EMD#3
41
リポケーション情報発行機関(RLE)
受信部#1
受信部#2
受信部#3
EMD I/F部
3
1
コンテンツ販売システム(CDS)
2
セキュアコンテンツサーバ(SMS)
リポケーション情報受信部
14
リポケーション情報格納部
16
音楽データ格納部
10
ライセンス格納部
9
秘匿領域ドライバ
7
宿帳格納部
8
ユーザI/F部
15
PD I/F部
5
メディアI/F部
6
12
記録再生装置(PD)
記憶メディア(PM)
13
記憶メディア(PM)
13

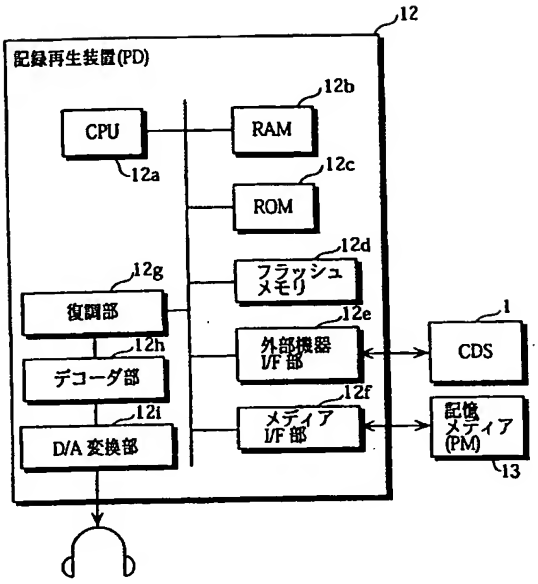
【図７】


12
記録再生装置(PD)
公開領域
121
公開ROM領域
122
123
公開R/W領域
秘匿領域
124

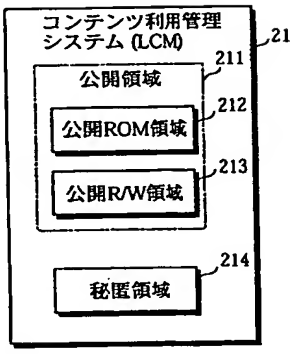
【図４】


132
公開ROM領域
RL－M
マスタリポケーション情報
0x4538A301773E0315
0x1345B64355FF9932
132a
公開ROM-W領域
RL－1
リポケーション情報Ⅰ
0x124576AC8088EB41
RL－2
リポケーション情報Ⅱ
0x84226A831005FF91

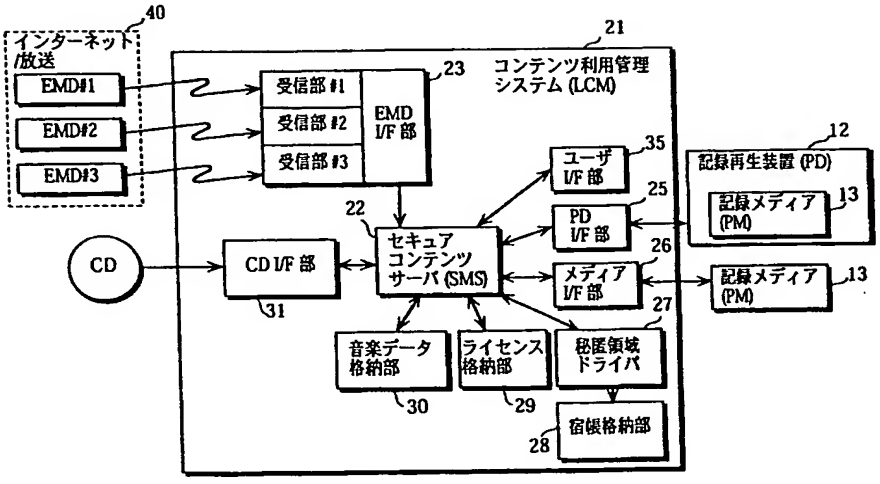
【図６】


12
記録再生装置(PD)
CPU
12a
RAM
12b
ROM
12c
フラッシュメモリ
12d
復調部
12g
デコーダ部
12h
D/A 変換部
12i
外部機器I/F部
12e
メディアI/F部
12f
1
CDS
記憶メディア(PM)
13

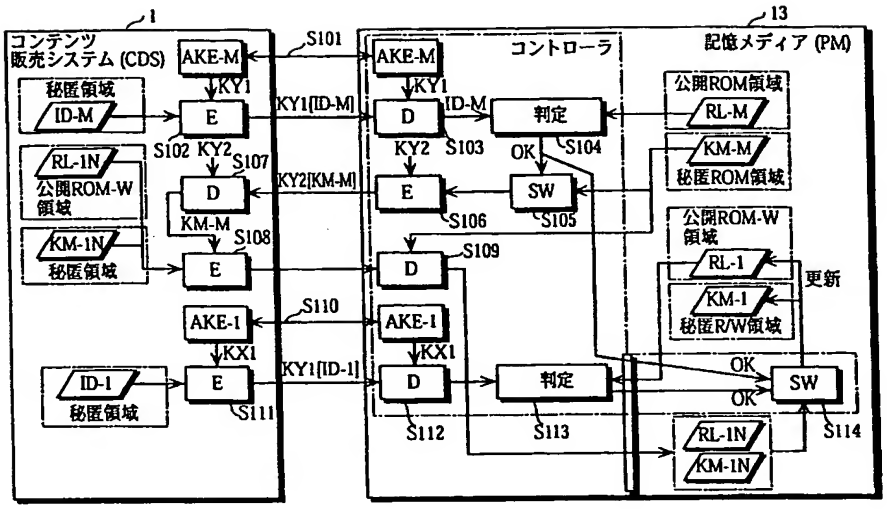
【図９】


コンテンツ利用管理システム (LCM)
21
公開領域
211
公開ROM領域
212
公開R/W領域
213
秘匿領域
214

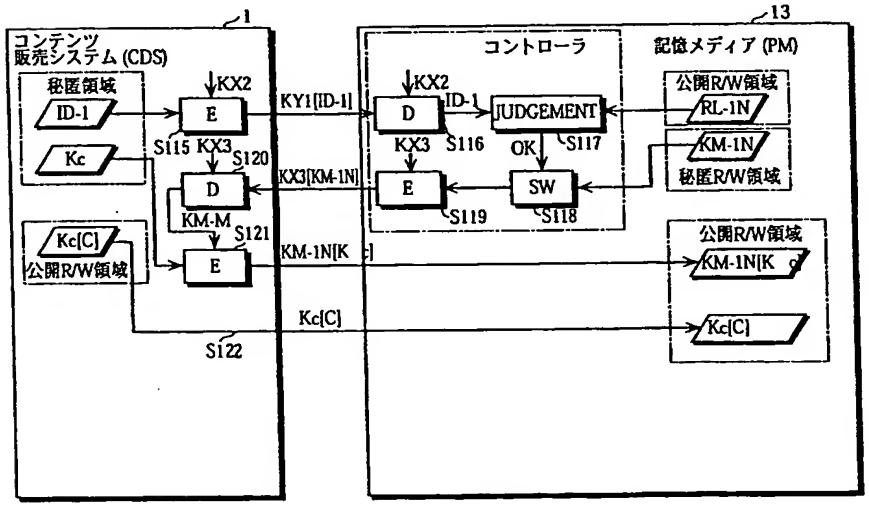
【図８】


40
インターネット/放送
EMD#1
EMD#2
EMD#3
21
コンテンツ利用管理システム (LCM)
受信部 #1
受信部 #2
受信部 #3
23
EMD I/F部
CD
CD I/F部
31
22
セキュアコンテンツサーバ (SMS)
ユーザI/F部
35
PD I/F部
25
メディアI/F部
26
12
記録再生装置 (PD)
記録メディア (PM)
13
記録メディア (PM)
13
音楽データ格納部
30
ライセンス格納部
29
秘匿領域ドライバ
27
宿帳格納部
28

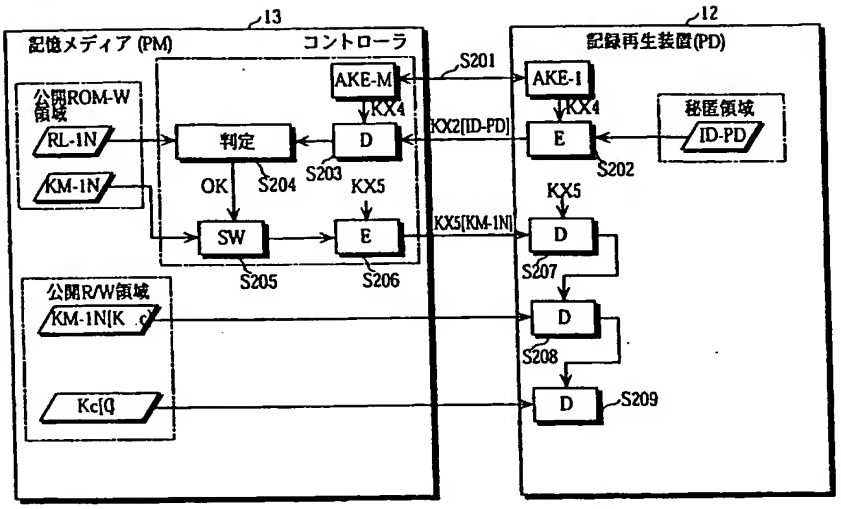
【図１０】


1
コンテンツ
販売システム (CDS)
AKE-M
KY1
秘匿領域
ID-M
E
S101
KY1[ID-M]
S102
KY2
S107
D
KM-M
RL-1N
公開ROM-W
領域
KM-1N
秘匿領域
KY2[KM-M]
S108
AKE-1
S110
KX1
ID-1
秘匿領域
KY1[ID-1]
S111
コントローラ
D
ID-M
判定
S103
S104
OK
E
SW
S106
S105
S109
D
AKE-1
KX1
D
判定
S112
S113
13
記憶メディア (PM)
公開ROM領域
RL-M
KM-M
秘匿ROM領域
公開ROM-W
領域
RL-1
更新
KM-1
秘匿R/W領域
OK
SW
OK
S114
RL-1N
KM-1N

【図１１】


1
コンテンツ
販売システム (CDS)
秘匿領域
ID-1
Kc
KX2
E
S115
KX3
S120
D
KM-M
Kc[C]
公開R/W領域
S121
E
KY1[ID-1]
KX3[KM-1N]
KM-1N[K
Kc[C]
S122
コントローラ
KX2
D
ID-1
JUDGEMENT
KX3
S116
OK
S117
E
SW
S119
S118
13
記憶メディア (PM)
公開R/W領域
RL-1N
KM-1N
秘匿R/W領域
公開R/W領域
KM-1N[K
Kc[C]

【図１２】



フロントページの続き

(51) Int. Cl.[7]　　識別記号　　F I　　ﾃｰﾏｺｰﾄﾞ(参考)
H０４L　9/32　　H０４L　9/00　　６７３Ｂ

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　小塚　雅之
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　廣田　照人
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　上林　達
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(72)発明者　田村　正文
東京都港区芝浦一丁目１番１号　株式会社東芝本社事務所内

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ BLACK BORDERS
- ☒ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLORED OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REPERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning documents *will not* correct images problems checked, please do not report the problems to the IFW Image Problem Mailbox